Department of Homeland Security Daily Open Source Infrastructure Report for 05 August 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

One Week Left −− Please Help Improve the DHS Daily Infrastructure Report!!

We are striving to improve the DHS Daily Infrastructure Report for all of our readers. Please help us in this effort by filling out a short feedback form, which can be found by clicking on this link:

http://chrome.osis.gov/questionnaire

The form will only be available for *one more week*, so please fill it out at your earliest convenience. Your participation is important to us! Thank you.

Daily Highlights

- Vnunet reports that according to the latest Experian−Gallup Personal Credit Index almost 20 percent of U.S. consumers admit to falling victim to identity theft, with younger adults at the greatest risk. (See item 12)
- The Associated Press reports the Federal Aviation Administration wants to restrict a wide swath of airspace over the Washington, DC area permanently, and make it a crime if a private pilot knowingly enters a zone that extends from Maryland to Virginia. (See item 18)
- The Associated Press reports more than 80 percent of California's buildings, power facilities, and other vital structures are in private hands, watched over by security guards many of whom are also being trained to watch out for terrorists. (See item 35)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 04, Reuters* — **OPEC output rises to highest since 1979.** Organization of the Petroleum Exporting Countries (OPEC) oil production rose 290,000 barrels per day in July to the highest level since December 1979 as Iraq boosted exports and the UAE restored output at oilfields after maintenance, a Reuters survey showed. Record crude oil prices have encouraged OPEC to push output to near 26−year highs. However, opening the taps has had little effect on prices. U.S. light crude as it a fresh record of $62.50 a barrel on Wednesday, August 3. "OPEC is producing as much crude oil as anybody wants," said Geoff Pyne, energy consultant for Standard Bank. "Refiners have no shortage of the grades they need. But it's out of OPEC's hands to bring the price down," said Pyne. Prices have rallied to records this year on concern that a stretched global refining system would struggle to meet rapidly growing fuel demand.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/04/AR2005080400196.html

2. *August 04, PJM Interconnection* — **PJM asks consumers in Mid−Atlantic region to conserve electricity.** PJM Interconnection, the electricity grid operator for the Mid−Atlantic region, requested that the public in the region conserve electricity on Thursday, August 4, while the area experiences a heat wave. Demand for electricity remains extremely high as a result of the continued hot and humid weather conditions. Adequate supplies of electricity are available. However, PJM is taking precautions to ensure the reliability of the transmission system during this time of heavy usage of the grid. While PJM expects to have enough electricity to meet the demand for power, if necessary the company may be required to initiate further operational procedures to preserve the reliable operation of the region’s electric power supply system. PJM is communicating about the situation with state government officials throughout the Mid−Atlantic region. PJM is coordinating efforts among generators, power suppliers and local utilities.
   Source: http://www.pjm.com/contributions/news−releases/2005/20050804−H−2−message−aug−4.pdf

3. *August 04, Sweetwater Reporter (TX)* — **New law will increase Texas renewable energy.** Texans will have the benefit of a significant growth in clean, economic renewable energy thanks to a new law signed by Governor Rick Perry. The law, Senate Bill 20, was passed in July during the first called session of the 79th Legislature. It expands the use of renewable energy in Texas over the next ten years, and takes steps to improve the electric transmission infrastructure for the benefit of all the state's renewable energy resources. Senate Bill 20 adds 3,000 megawatts to the current 2,880 megawatt 2009 Goal for Renewable Energy and extends the date to 2015.
   Source: http://sweetwaterreporter.com/articles/2005/08/04/news/news3 .txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *August 04, The News−Press (FL)* — **Florida chemical spill causes street closings.** A chemical spill of sulphur dioxide at the Myers Central Wastewater Plant in Fort Myers, FL, wastewater treatment plant sent two workers to the hospital Thursday, August 4, causing street closings and warnings to residents to stay indoors. This occurred when two licensed workers were attempting to move an empty tank of sulphur dioxide; the tank separated from the valve it was attached to and the sulphur dioxide began to escape. The workers were not believed to be seriously injured. A fire department Hazmat team plugged the leak and the spill was contained within about an hour. "If inhaled in a very concentrated amount it could be deadly," said Jennifer Hobbic, a spokesperson for the City of Fort Myers. Police closed Raleigh and Billie streets to traffic for about an hour and told nearby residents to stay in their homes.
Source: http://c.moreover.com/click/here.pl?j364769799&f=25000003004 60

5. *August 04, Roanoke Times (VA)* — **Plant fire closes down streets.** A fire broke out in an air duct at the Hooker Furniture Corporation plant in the 2000 block of Greenbrier Avenue Wednesday evening, August 3, prompting the evacuation of the plant's evening shift. Workers evacuated the plant soon after the fire was reported and did not return after it was put out, said Tiffany Bradbury, a spokesperson for the Roanoke Fire−Emergency Medical Services Department. A sprinkler system in the building contained the fire, which started in the paint booth, before firefighters were able to extinguish it within 20 minutes. No one was injured, Bradbury said. As of Wednesday night, fire investigators were still trying to determine what caused the fire, which caused roughly $5,000 in damage, she said. Before the fire was put out, authorities closed off streets around the plant's red brick building and called out a city Hazmat truck in case any of the chemicals used at the plant became involved in the blaze.
Source: http://www.roanoke.com/news/roanoke%5C28826.html

6. *August 04, Associated Press* — **Fire at chemical company in Pennsylvania forces residents to evacuate.** A fire at the Centre Chemical Company in Bellefonte, PA, caused extensive damage Wednesday night, August 3, and forced the evacuation of more than 25 homes. The building is believed to have contained janitorial supplies and cleaning agents, but no hazardous materials. The fire was brought under control by midnight. An investigation into the cause of the fire was made Thursday, August 4.
Source: http://www.whptv.com/news/state/story.aspx?content_id=946A8A59−2E34−45F9−A08E−123105FF33DF

7. *August 04, Associated Press* — **Michigan highway closed after tanker catches fire.** A tanker truck carrying 12,000 gallons of gasoline caught fire and closed down part of a northern Michigan highway. Crews say the tanker went up in flames just before early Thursday morning, August 4, on US−31 in Grant Township, MI. Police believe the tanker's brakes may have overheated, sparking the fire. At first, the driver tried putting out the flames himself, but it quickly spread out of control. Flames could be seen shooting at least 200 feet into the air. The fire knocked down power lines and knocked out power out for 80−100 people. Five nearby homes were evacuated. Doctors treated two elderly people for smoke inhalation, but no one else was hurt. Part of US−31 remains closed because the heat severely damaged the road.
Source: http://www.wluctv6.com/Global/story.asp?S=3681860

8. *August 04, KHQ−TV (WA)* — **Two homes in Washington neighborhood evacuated after gas line break.** Residents of two homes in the Seven Mile area northwest of Spokane, WA, were evacuated for a few hours Thursday morning, August 4, because of a gas line break. The leak occurred east of Sundance Golf Course and Highway 291 at 10502 North Jimmy Road. Washington State Patrol trooper Jim Hayes said that Avista Utilities crews responded very quickly to squelch the leak. No injuries are reported.
Source: http://www.msnbc.msn.com/id/8827010/

9. *August 03, Indy Channel News (IN)* — **Gas line leak forces resident evacuations.** Sixty residents in a Cicero, IN, were evacuated Wednesday, August 3, after a gas line leading into their subdivision was broken by a company who had been installing fence posts and accidentally hit the line. The break affected close to 200 homes. Workers worked for almost three hours to fix the line.
Source: http://www.theindychannel.com/news/4805642/detail.html

10. *August 02, WTVQ (KY)* — **Chlorine leak causes evacuations around Kentucky plant.** Employees at the Clark County, KY, wastewater treatment plant discovered the plant's chlorine regulator was leaking on Tuesday, August 2. The building was immediately evacuated, but one worker who inhaled the gas fumes was rushed to the hospital and treated for irritation in his nose and throat. Fire and Hazmat crews ordered the evacuation of a quarter mile area around the plant. No homes or businesses were affected, but a dozen workers at a nearby construction site had to leave the job due to their close proximity to the plant. It took firefighters about three hours to seal the leak and check for dangerous fumes. Once the chlorine had dissipated, the plant was reopened.
Source: http://www.wtvq.com/servlet/Satellite?pagename=WTVQ/MGArticle/TVQ_BasicArticle&c=MGArticle&cid=1031784208754&path=

11. *August 01, Associated Press* — **Wrong type of pipe caused Texas plant explosion, British Petroleum says.** The installation of the wrong type of pipe spool at a Texas City, TX, refinery is believed to have caused last week's explosion and fire at the same British Petroleum (BP) plant where 15 people were killed in March, company officials said Monday, August 1. An eight−inch section of heavy steel pipe, located between a compressor and heat exchanger on the Resid Hydrotreater Unit, failed on Thursday, July 28. No one was injured during the resulting blast and blaze. The section failed because workers installed the wrong type of steel pipe spool on the outlet of the heat exchanger, BP spokesperson Ronnie Chappell said. The elbow−shaped pipe spool, believed to have been mistakenly installed when the unit underwent routine maintenance in February, is not designed to withstand higher temperatures. "Figuring out what occurred was relatively easy. The question now is how did that error occur, given we have pretty elaborate processes and procedures which govern this kind of work," he said. The investigation is expected to take two weeks. Investigators with the U.S. Chemical Safety and Hazard Investigation Board are conducting their own probe into the most recent accident.
Source: http://www.signonsandiego.com/news/business/20050801−1739−pl antexplosion.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

12. *August 04, Vnunet* — **Experian−Gallup report warns of growing danger.** Almost 20 percent of U.S. consumers admit to falling victim to identity theft, and younger adults are at greatest risk, according to the latest Experian−Gallup Personal Credit Index published Thursday, August 4. Twenty−five percent of consumers across America under the age of 30 admitted to having their financial information stolen, compared with about 18 percent in the middle−aged group and just 11 percent among consumers 65 and older, the study found. About two−thirds of consumers who have not experienced identity theft consider that it is unlikely to happen to them. Only six percent have purchased some form of identity theft protection, and just four percent have purchased identity theft insurance and checked their credit report to see whether they have been victims of identity theft. Although few consumers have taken preventive action to avoid becoming a victim of identity theft, 62 percent said they were concerned that their financial information could be stolen online. More than half are also concerned that their personal information could be stolen from the post office (55 percent) or at a shop (53 percent), while 47 percent fear becoming a victim at a restaurant.
    Experian−Gallup Personal Credit Index:
    http://www.nationalscoreindex.com/?sc=300001&bcd=epshp
    Source: http://www.vnunet.com/vnunet/news/2140768/identity−theft−gal lup−experian

13. *August 03, Denver Post (CO)* — **University of Colorado seeking help to evaluate hacked system.** The University of Colorado (CU) will hire a computer−security company to audit its technology safeguards after hackers broke into the system three times in two weeks, officials said Tuesday, August 2. CU also plans to put firewalls on some of its 26,000 computers that are now accessible to the public. A team from Applied Trust Engineering, which has been scanning CU files since computer breaches were discovered July 14, noticed some suspicious files July 27, said Larry Drees, Buff OneCard program director. The team created an image of the hard drive that was hacked, and the server was disconnected from the network. Computer scientists continue to analyze the image of the hard drive to see what the hacker might have retrieved. That information could help determine whether the hacker wanted to use the system to access sensitive information, said Dan Jones, information−security coordinator. It's also possible, though unlikely, the hacker could use the information to make fake Buff OneCards, Drees said. Just in case, CU began replacing Buff OneCards on Tuesday, August 2, and plans to replace them all within 30 to 40 days, according to Drees.
    Source: http://www.denverpost.com/search/ci_2909173

14. *August 03, WFAA−TV (TX)* — **Large identity theft ring arrested in North Texas.** Police in North Texas have broken up an identity theft ring Wednesday, August 3, that led to the purchase thousands of dollars in merchandise with stolen credit card numbers. Police filled two patrol cars full of documents that had been seized at a gas station along Interstate 20. A former employee there allegedly stole more than 600 credit and debit card numbers, and then attempted to make more than $21,000 in online purchases using two computers −− also taken by police as evidence. Authorities in Forest Hill, TX, said it's one of the biggest identity theft rings ever busted in the region.

Source: http://www.wfaa.com/sharedcontent/dws/wfaa/latestnews/stories/wfaa050803_am_idtheft.3a9d15ce.html

15. *August 03, UNISYS* — **United Kingdom market ripe for fraud.** Survey results from Unisys Corporation released Wednesday, August 3, reveal that United Kingdom (UK) consumers' apathetic attitude to fraud could be helping to perpetuate the rapidly growing identity theft industry, which is now estimated to be costing UK businesses $2.3 billion per year. The independent study, commissioned by Unisys, surveyed 1,000 UK households to investigate the incidence of and attitudes towards financial fraud. The findings revealed that more than one in ten UK consumers (11 percent) have now been the victims of fraud. Despite these statistics, 61 percent of respondents stated that they have no concerns about the safety of their money kept in their bank. The research reveals that despite the high incidence of identity theft, most consumers are not interested in proactively helping to manage the risk of fraud. Fifty−eight percent of respondents surveyed admitted that they had no desire to be educated about banking security or fraud protection. Fifty percent of consumers would not switch their bank to obtain better security or protection. Consumers also showed low levels of interest for additional security services. Sixty−six percent of respondents declined when asked if they would pay for better fraud protection.
Source: http://www.unisys.co.uk/about__unisys/news_a_events/08038564 .htm

16. *August 03, NBC6 (FL)* — **Wachovia Bank warns customers of possible identity theft.** Thousands of Wachovia Bank customers will receive a letter stating that their identities might have been stolen after computer hackers broke into another company's computer system, bank officials said. Wachovia representatives said it was not the bank's security system but the system of another company, Card Systems Solutions, Inc. that was hacked. As a result, some customers' Visa Check Card numbers, names and other information might have been exposed. Card Systems Solutions, Inc. is not affiliated with Wachovia; the company processes check and credit card transactions for banks. Wachovia representatives said the bank is reissuing thousands of check cards to customers who may have had their identities stolen. Bank representatives said customers should also double check their accounts by looking online or calling Wachovia to make sure there are no unusual transactions.
Source: http://www.nbc6.net/money/4805531/detail.html

[Return to top]

Transportation and Border Security Sector

17. *August 04, Agence France−Presse* — **Bogus Air France captain picked up at main Paris airport.** Police at Charles de Gaulle airport at Roissy, north of Paris, said Tuesday, August 2, they had detained a man wearing the uniform of an Air France captain and seeking information about flight departures. He and another man were detained as they were driving away from the airport. The man wearing the uniform, as well as an access badge in the name of his companion, went to the Air France desk and asked about departing flights and passenger numbers. He also tried to get a ticket handed over. The agent at the desk, surprised by the unusual behavior, refused and the fake captain left in a car the number of whose plate was noted. The car was stopped in the area surrounding the airport and a second man discovered and arrested. Police have identified the two men, aged between 35 and 40 and resident in the Paris

region. Their home was due to be searched.
Source: http://www.usatoday.com/travel/news/2005−08−03−bogus−captain_x.htm

18. *August 04, Associated Press* — **FAA proposes permanent restrictions over Washington, DC.** The government wants to restrict a wide swath of airspace over the Washington area permanently and make it a crime if a private pilot knowingly enters a zone that extends from Maryland to Virginia. Pilots have strayed hundreds of times since the government temporarily restricted airspace over the capital just before the start of the Iraq war in 2003. In many cases, fighter jets, which are prepared to shoot down a plane, have escorted an errant aircraft to an airport. The restricted airspace includes an outer ring that has a radius of about 30 to 45 miles and an altitude of 18,000 feet. A plane that flies into this zone must file a flight plan, emit a special signal so air traffic controllers can follow it and maintain radio contact with the ground. An inner ring extends about 15 miles from the Washington Monument. Most flights are prohibited from flying into this area. The Federal Aviation Administration (FAA) proposal would allow the government to impose criminal penalties −− fines and up to a year in prison −− on anyone who knowingly or willingly enters the outer zone.
FAA Document: Washington DC Metropolitan Area Special Flight Rules Area: http://dms.dot.gov/search/document.cfm?documentid=341297&doc ketid=17005
Source: http://www.usatoday.com/travel/flights/2005−08−03−faa−dc_x.h tm

19. *August 04, Star Tribune (MN)* — **Sun Country pilot kept off flight after flunking alcohol test.** A Sun Country Airlines pilot was prevented from flying to San Francisco on Friday, July 29, after testing above the legal limit for alcohol. Michael B. Schuster, 39, was stopped by security officers at Minneapolis−St. Paul International about 7:20 p.m. (CDT), after they smelled alcohol on his breath and saw what they described as bloodshot eyes. Schuster has been suspended, said Shaun Nugent, company chief executive officer. Nugent said the company "has a zero tolerance policy for drugs and alcohol, and, consequently, the employee is suspended." He said the FAA has taken over investigation of the case. Schuster was not arrested because he did not actually take control of the airplane.
Source: http://www.startribune.com/stories/462/5543458.html

20. *August 04, Globe and Mail (Canada)* — **Pearson airport security measures solid, executive says.** As some of the 309 bewildered passengers and crew on an Air France jet scrambled across an airport perimeter fence and ran onto the neighboring highway, the question arises: If they could pass through freely, is security tight enough around Canada's busiest airport to guard against intruders? Brian Lackey, vice−president of operations and chief engineer at the Greater Toronto Airports Authority, firmly stands behind Pearson International Airport's security measures. Around the perimeter, there may be an unmonitored two−meter high chain−link fence to delineate airport property. But to keep trespassers out, a three−meter chain−link fence with coiled barbed wire at the top encircles the airport and is monitored by cameras 24 hours a day, he said. Lackey said the Air France Airbus A−340 plane skidded off the runway, was consumed by flames and plowed through the main security fence. As a result, passengers −− who were evacuated from the plane quickly −− had to get across only the unmonitored perimeter fence. "To keep people out, it's very effective. To keep planes out, not very," Lackey said yesterday of the security fence. But immediately after the plane broke through the security fence, alarms sounded.
Source: http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/L

AC/20050804/PLANEFENCE04/TPNational/Canada

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

21. *August 04, Statesman Journal (OR)* — **Blackberry harming fungus is in 14 counties.** A fungus that harms commercially grown evergreen blackberries, as well as unwanted Himalayan blackberries, has swept across Western Oregon. The number of Oregon counties in which the fungus −− a species called Phragmidium violaceum −− has been detected has doubled to 14 in just a few weeks, Oregon Department of Agriculture officials said Wednesday, August 3. Before this year, Phragmidium violaceum never had been found in North America. Oregon's famed Marion blackberries are safe from fungus, but it threatens the evergreen blackberry crop. Some evergreen blackberry growers expect that their yields will be trimmed by 30 percent to 50 percent, agriculture officials said. The fungus leaves purple spots on the tops of blackberry leaves with corresponding yellow and black pustules underneath the leaves. As it develops, the fungus causes foliage to dry up and stop growing. The plant disease has attacked blackberries in the heart of the Willamette Valley, showing up in Marion, Polk, Yamhill, Clackamas, Multnomah, Linn, Benton, and Lane counties.
Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20050804/BUSINESS/508040333/1040

22. *August 04, Associated Press* — **Chile crop hit by virus.** Chile growers in the Mesilla Valley and Rio Grande corridor have seen a 20 to 25 percent crop loss due to curly top, said Stephanie Walker, extension vegetable specialist at New Mexico State University. Researchers had feared the losses would be much worse. “2001 was a disaster for chile crops due to curly top. We realized that this year, we had the potential for it to be that serious again. We were ready for battle,” said Walker, referring to the curly−top attack four years ago that reduced chile crops by 30 percent to 50 percent across Doña Ana and Luna counties. Diligence and quick measures taken by chile farmers proved key in controlling the virus, she said. “Some growers will have reduced yields, but it’s not going to hurt contracted acreages,” Walker said. She said the rates of curly−top infection vary across the state, but chile fields in the eastern and western parts of New Mexico were not significantly affected. Curly top stunts the growth of chile plants, causing them to produce only one or two peppers of poor quality and taste. The virus also can kill chile and tomato plants.
Source: http://www.freenewmexican.com/news/30878.html

23. *August 03, Associated Press* — **Agency floats plan to deal with chronic wasting disease.** The Montana state Fish, Wildlife, and Parks Department has issued a draft management plan for dealing with chronic wasting disease (CWD). So far, no wild animals in Montana have come down with the disease, although it did show up in 1999 in elk at a game farm near Philipsburg.

The disease has since been found in wild animals within 100 to 150 miles of the state line in Saskatchewan, Canada, Wyoming, and South Dakota. The most relaxed plan calls for doing nothing other than surveillance in parts of the state most likely to see the first CWD case. A more aggressive plan would stiffen laws dealing with feeding and baiting deer and elk, end the sheltering of orphaned deer and elk fawns, and ban imports of certain parts of deer and elk hunted outside the state. If the disease shows up, the plan calls for testing animals in a designated "high−risk zone" near where the first case is found. If more than five percent of the animals tested have CWD, half of all the animals in the area would be destroyed. The most aggressive plan calls for killing every deer and elk within at least 80 square miles around where the first positive case is found.
Source: http://rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_3972935,00.html

24. *August 03, StopSoybeanRust.com* — **Defoliation and copious sporulation by rust in new Georgia find.** Soybean rust was found Wednesday, August 3, for the first time at the Ponder Research Farm on the Coastal Plain Experiment Station in Tift, GA, at a level termed "epidemic" due to the amount of defoliation and spore production at the location. According to the Georgia state commentary by Bob Kemerait, "Epidemic is established at Ponder Farm in Tifton. Recent weather patterns appear to have favored spread of rust. Soybean growers on the Coastal Plain should be willing to spray fungicide as crop reaches reproductive development." Soybean rust was confirmed in Tift County on July 18 on a soybean leaf in a sentinel plot in the county.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=487

[Return to top]

Food Sector

25. *August 03, American Society for Microbiology* — **Research opportunities in food and agriculture microbiology.** A new report, released by the American Academy of Microbiology, details the ever−present threats to the food supply posed by disease, spoilage, and the specter of agroterrorism, along with how the commitment to research in food and agricultural microbiology is on the decline. "The constant spread and evolution of agricultural pathogens provides a continually renewed source of challenges to productivity and food safety. However, research support over the last few decades has been lean and is, in fact, decreasing," says Michael Doyle of the University of Georgia, a co−author of the report. Trouble recruiting and maintaining graduate students is also harming programs and will ultimately affect the field, says Doyle. "Reversing the decline in funding and recognition of the value of agricultural research requires fundamental changes, in addition to an infusion of financial support." Microorganisms continue to cause harm to the food supply beyond the farm, causing spoilage and, in some cases poisoning and disease. Additionally, the global movement of agricultural products, industrial agricultural processes, and the potential for malicious release of pathogens by bioterrorists add new vulnerabilities. In addition to the threats, microorganisms can also benefit the food supply, helping to preserve foods or acting as probiotics.
Source: http://www.asm.org/ASM/files/ccLibraryFiles/FILENAME/000000001684/AgriFoodMicrobiology.pdf

[Return to top]

Water Sector

26. *August 03, Las Vegas Sun* — **Report: EPA should update nuclear levels for drinking water.** The Environmental Protection Agency (EPA) should revise its 29−year−old standard for radioactive materials in drinking water, according to a report released on Wednesday, August 3. In general, the nation's drinking water is safe from radioactive contamination, said the report's author, Arjun Makhijani, president of the Maryland−based Institute for Energy and Environmental Research. However, radioactive materials could endanger water sources near former government nuclear weapons facilities, Makhijani said. The federal drinking water standard for allowable levels of materials like plutonium−239, an atomic bomb ingredient, is too lax, Makhijani said. The report recommends that the EPA set a standard that is 100 times more strict, especially as the government continues clean−up efforts at former nuclear weapon sites. Clean−up efforts include enclosing radioactive waste, including plutonium, in tanks, but the waste is still left near vital water sources, Makhijani said. An EPA spokesperson said that the agency reviews its standard every six years. "Unless someone has significant information not previously available, there is not a compelling case to change the rule," EPA spokesperson Dale Kemery said.
Report: http://www.ieer.org/reports/badtothebone/fullrpt.pdf
Source: http://www.lasvegassun.com/sunbin/stories/lv−gov/2005/aug/03 /519150852.html

[Return to top]

Public Health Sector

27. *August 04, Associated Press* — **West Nile virus screening reportedly succeeding.** Screening blood donations for the West Nile virus to prevent its spread has proved remarkably effective, though a few contaminated units have been missed. The U.S. blood supply has been screened for West Nile virus since the summer of 2003, after it became apparent that the mosquito−borne illness could be passed on through transfusions. Since then, West Nile infections have been found in 1,039 of the 27 million blood donations screened, according to the U.S. Centers for Disease Control and Prevention (CDC). That means about 1,500 transfusions of tainted−blood products were prevented, said the CDC's Lyle Petersen. Petersen estimated that screening has reduced the risk of getting an infection through a blood transfusion by 90 percent. The virus that is missed is present in very low levels, he said. The number of confirmed cases of West Nile infections through blood transfusions dropped significantly once screening began. There were 23 confirmed cases in 2002, six in 2003, and only one last year, according to CDC figures.
Source: http://www.chicagotribune.com/news/nationworld/chi−050804019 4aug04,1,6246562.story?coll=chi−newsnationworld−hed&ctrack=1 &cset=true

28. *August 03, Academic Emergency Medicine* — **Knowledge of smallpox diagnosis among D.C. emergency physicians assessed.** Researchers sought to assess the current knowledge of full−time emergency physicians in Washington, DC, regarding the initial diagnosis of smallpox and the initial care of the patient with smallpox. Researchers prepared a written true/false test based on information accessed from the current U.S. Centers for Disease Control and Prevention (CDC) Website on smallpox. The 20−question test was administered to full−time

emergency physicians practicing emergency medicine in all seven adult civilian hospitals in Washington, DC. The overall response rate was 81 percent. The average score was 59 percent correct. Physicians were most likely to know that the symptoms of smallpox begin with a two to four day prodrome of fever and myalgia; that no antiviral treatment is of more proven value than vaccination of contacts; and that a person with smallpox may be contagious before any rash appears. Physicians were least likely to know that when dealing with a known case of smallpox, masks are not needed by treating personnel if they have been vaccinated; that the rash of smallpox begins with 24–48 hours of flat, erythematous macules; and that very typically the rash of smallpox begins in the mouth.
Source: http://www.aemj.org/cgi/content/abstract/12/8/771

29. *August 03, Associated Press* — **Humans dying of pig disease a concern.** Experts on a Streptococcus germ that's sickening people and pigs in China are baffled by reports of 38 farmers suddenly falling ill, bleeding under the skin, and dying −− all previously unheard of with the disease. While not uncommon in pigs, Streptococcus suis is seldom seen in people and never dozens of cases all at once −− raising bigger questions about whether the germ has mixed with some other bacteria or virus. "Something is different," Marcelo Gottschalk, who works in the world's only reference laboratory for Streptococcus suis at the University of Montreal in Canada, told The Associated Press. So few people have studied this disease, he's unsure how the Chinese have been able to identify it and what type of vaccine they plan to use since immunizations typically are not effective. Chinese state media have reported that enough vaccine for 350,000 pigs has already been sent to Sichuan province and that enough doses for 10 million swine will be shipped later. Gottschalk said Streptococcus suis usually takes a while to develop in people and cases are typically few and far between. China has reported more than 200 confirmed or suspected human cases since June. The World Health Organization and the U.N. Food and Agriculture Organization have questioned whether Streptococcus suis could possibly have combined with some other disease or bacteria in China.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/03/AR2005080301392.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *August 04, Beatrice Daily Sun (NE)* — **Nebraska responders train for emergencies.** A simulation and evaluation drill took place Wednesday, August 3, at the Beatrice Speedway in Beatrice, NE, that involved members of Beatrice Fire and Rescue, Gage County Emergency Management and the Nebraska National Guard Weapons of Mass Destruction Civil Support Team at the Gage County Fairgrounds. The drill started when a suspicious white powdery substance was found in the press box. In use was multi−million dollar equipment owned by the civil support team, a full−time, federally funded Nebraska National Guard Unit established to

support local first responders in the event of a terrorist attack. The team, which is on call 24 hours a day, seven days a week, brought their 22 members and 12 vehicles down from Lincoln for a simulation of an attack during race day at the Gage County Fairgrounds. The drill included identification of the powdery substance as well as the discovery of contaminated food in the kitchen and a toxic mist in the men's room. The drill functioned as part of a weeklong evaluation for the CST, which has spent the last 18 months in training and will be ready to respond to a real emergency once the evaluation is complete, Meints said.
Source: http://www.beatricedailysun.com/articles/2005/08/04/news/new s1.txt

[Return to top]

Information Technology and Telecommunications Sector

31. *August 03, IDG News Service* — **Cisco passwords reset after Website exposure.** Cisco Systems Inc. is resetting passwords for all registered users of its Cisco.com Website after discovering a vulnerability in its search engine software that left user passwords exposed, the company said Wednesday, August 3. The passwords are used by Cisco customers, employees and partners who have registered on the Website to get access to special areas of the site or to receive e−mail alerts, said Cisco spokesperson John Noh. Cisco was made aware of the problem early Monday and corrected it immediately, Noh said. As a precaution, the company is now in the process of sending out new passwords to all registered users of Cisco.com, who will be unable to access password−protected areas until they receive their new passwords, Noh said. Noh could not say how long it will take to send out all of the new passwords. The vulnerability could not be exploited to gain access to sensitive information like Cisco's source code, he said. "We do not believe any sensitive data were compromised as a result of this."
Source: http://www.computerworld.com/developmenttopics/websitemgmt/s tory/0,10801,103661,00.html

32. *August 03, CNET News* — **Internet servers at risk of attack.** In a scan of 2.5 million so−called Domain Name System machines, which act as the White Pages of the Internet, security researcher Dan Kaminsky found that about 230,000 are potentially vulnerable to a threat known as DNS cache poisoning. "That is almost 10 percent of the scanned DNS servers," Kaminsky said in a presentation last week at the Black Hat security event in Las Vegas, NV. The motivation for a potential attack is money, according to the SANS Internet Storm Center, which tracks network threats. Attackers typically get paid for each spyware or adware program they manage to get installed on a person's PC. Information lifted from victims, such as social security numbers and credit card data, can also be sold. Additionally, malicious software could be installed on a PC to hijack it and use it to relay spam. The DNS servers in question are run by companies and Internet service providers to translate text−based Internet addresses into numeric IP addresses. The cache on each machine is used as a local store of data for Web addresses.
Source: http://news.com.com/DNS+servers−−an+Internet+Achilles+heel/2 100−7349_3−5816061.html?tag=nefd.lede

33. *August 03, Techworld* — **Key management holding back encryption.** Businesses are keener than ever to roll out data encryption, but are still struggling with the complexity of key management, a new survey has concluded. The survey was carried out by UK encryption

specialist nCipher, sampling 237 "decision makers" at large enterprises across the globe. The main problem appears to be key management with nine percent of those surveyed having more than 10,000 keys on servers, and 11 percent having the same number on desktops. Further down the scale, 16 percent had 1,000 keys on servers, with almost a quarter having the same number of desktops. Underscoring this issue, 31 percent of managers with 500 or more keys in their organizations admitted they knew little or nothing about available key management systems. The survey found that encryption is rapidly becoming a mainstream technology, with its use now mandated across a wide range of applications. Drivers included government legislation, and private sector date protection standards developed by groups such as the Payment Card Industry.
Survey: http://www.ncipher.com/crypto2005
Source: http://www.techworld.com/security/news/index.cfm?NewsID=4150&Page=1&pagePos=2

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: A presentation at Defcon entitled "Live penetration Test of the Backbone" was scheduled to include use of an exploit disclosed by Michael Lynn earlier this week. The exploit is NOT the weak version demo'd by Lynn, but a fully working version that is capable of re−routing traffic, man in the middle and / or dropping the router. EFF lawyers toned down the presentation to avoid ISS and/or Cisco lawsuits. Analysis: There is an exploit. It will fall into the wrong hands. Prepare your Networks. RECOMMENDATIONS AND COUNTERMEASURES If your network doesn’t need IPv6, disable it. This will eliminate exposure to this vulnerability. On a router which supports IPv6, disable it by issuing the command "no ipv6 enable" and "no ipv6 address" on each interface. On those systems that do require IPv6 capabilities check the Cisco advisory information to determine vulnerability and countermeasures.
http://www.cisco.com/warp/public/707/cisco−sa−20050729−ipv6. shtml

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 6881 (bittorrent), 80 (www), 445 (microsoft−ds), 139 (netbios−ssn), 135 (epmap), 53 (domain), 25 (smtp), 1434 (ms−sql−m), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

34. *August 04, USA TODAY* — **Surveillance in Madison County.** Engineers at Iowa State University are working to shelter the venerable covered bridges from vandalism by using high−tech surveillance. There were once 19 bridges in Madison County. Only five remain, all listed on the National Register of Historic Places. Several have been vandalized in recent years, and researchers at Iowa State are developing remote monitoring devices to prevent further damage. The Iowa State team received $126,000 from the U.S. Department of Agriculture's Forest Product Laboratory to develop and install a monitoring system for one of the bridges. After that, county officials will assess the benefits and decide if it should be installed on the remaining bridges. The system is in three parts: •Flame detection. These devices will detect ultraviolet light, infrared light and the flicker rate as light frequencies change. •Infrared cameras. This camera detects heat rather than light and will be able to photograph people on the bridge even at night. •Fiber−optic strain gauges. These will be imbedded to react to changes in temperature. The researchers plan to have the work done on the first bridge by summer's end. They will test the system by staging mock arson and vandalism scenarios with law enforcement officials.
Source: http://www.usatoday.com/travel/news/2005−08−03−madison−bridg es_x.htm

35. *August 04, Associated Press* — **Private security guards' training boosted in anti−terror effort.** More than 80 percent of California's buildings, power facilities and other vital structures are in private hands, watched over most closely by security guards on the lookout mainly for burglars, vandals and shoplifters. Now many are also being trained to also watch out for terrorists. The state Department of Consumer Affairs last month began requiring licensed security guards' training to include a section on what to look for and whom to alert if they see a mysterious package, someone dressed inappropriately for the season, a person taking pictures of a facility or any other suspicious activity. Steve Giorgi, who helped develop the curriculum as a deputy director at the Department of Consumer Affairs, which licenses guards. Giorgi is also a former deputy director for the state Office of Homeland Security. Guards who are currently employed also will get the training, which includes sections on potential terrorist weapons, weapons of mass destruction, and how to respond in the event of a terrorist attack. "This is basically 400,000 additional eyes and ears out there to observe suspicious activity," compared to about 90,000 sworn law enforcement officers in California, Giorgi said. "Cameras and security officers in the right place really can make a difference."
Source: http://www.taftmidwaydriller.com/articles/2005/08/03/news/fe atures/feat02.txt

[Return to top]

General Sector

36. *August 04, New York Times* — **Al Qaeda leader warns Great Britain and U.S. in new videotape.** One of the top leaders of al Qaeda, Ayman al−Zawahiri, warned Britons in a videotaped message Thursday, August 4, of more attacks and said that the U.S. would witness "horrors" the likes of which it had not experienced in Vietnam. The tape was broadcast on the Arabic language station Al Jazeera and excerpts were published on the station's Website. The timing of the threats was relevant following two attacks last month in London, England and

Sharm al−Sheikh, Egypt. The remarks did not say al Qaeda was behind the London bombings. While a connection between the attacks and the group has been explored but not established, some officials have suggested that the ideology of the group might be helping inspire attacks through a violent interpretation of Islam. Zawahiri and Osama bin Laden are the top two leaders of al Qaeda. Both men have been in hiding for nearly four years, and many of the group's commanders have been captured or killed. According to the Web excerpts, Zawahiri said that the policies of Prime Minister Tony Blair were to blame for the attacks on Britain and that the U.S. would bring more attacks on itself as well with its "policies of aggression against Muslims."
Source: http://www.nytimes.com/2005/08/04/international/europe/04cnd −tape.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer